REMARKS

Claims 1-3, 5-24, 26-28, 50-51 and 53-68 are pending in the present application. Claims 1, 11, 14, 19, 22, 26, 50, 51, 57, 59, 61, 63, 65 and 67 have been amended, and Applicants respectfully request allowance of the present application in view of the arguments set forth herein below.

The amendments to claims 1, 14, 22 and 50 find support in at least paragraphs [0038]-[0039] and FIGURE 2 of the application publication. The amendments to claims 11, 19, 26 and 51 find support in at least paragraph [0034] of the application publication. Finally, the amendments to claims 57, 61 and 65 simply add recitations found in the previously filed dependent claims 59, 63 and 67, respectively. Also, the amendments to claims 59, 63 and 67 are made in view of the amendments to their respective parent claims.

Claim Rejections – 35 USC § 103

The Office Action rejected claims 1-3, 5-9, 11-14, 16-24, 26-28, 50, 51 and 53-68 under 35 U.S.C. §103(a) as being allegedly obvious over various references. These rejections are respectfully traversed in their entirety.

The Office has the burden under 35 U.S.C. § 103 to establish a prima facie case of obviousness. *In re Piasecki*, 745 F.2d 1468, 1471-72, 223 USPQ 785, 787 (Fed. Cir. 1984). To establish a prima facie case of obviousness, four basic criteria must be met. Obviousness is a question of law based on underlying factual inquiries, which inquiries include: (A) determining the scope and content of the prior art; (B) ascertaining the differences between the claimed invention and the prior art; (C) resolving the level of ordinary skill in the pertinent art; and, if applicable, and (D) secondary considerations. *Graham v. John Deere Co.*, 383 U.S. 1 (1966). Any differences between the prior art and the claims at issue must be such that they would have been obvious to a person having ordinary skill in the art at the time the invention was made. *KSR Int'l Co. v. Teleflex Inc.*, 127 S. Ct. 1727, 1734, 167 L.Ed.2d 705, 75 USLW 4289, 82 U.S.P.Q.2d 1385 (2007).

Claims 50 and 56

The Office Action rejected claims 50 and 56 under 35 U.S.C. §103(a) as being allegedly obvious over U.S. Patent No. 6,782,103 (hereinafter "Arthan et al.") in view of U.S. Publication No. 2002/0071561 (hereinafter "Kurn et al."). These rejections are respectfully traversed in their entirety.

Applicants respectfully submit that claims 50 and 56 are not obvious in view of the cited references under a *Graham* analysis. More specifically, the combination of Arthan et al. with Kurn et al. fails to teach or suggest all of the limitations of claims 50 and 56, and one of ordinary skill in the art would not arrive at the limitations of claims 50 and 56 in view of the differences between these references and the presented claims.

A. Scope of the Prior Art

Arthan et al. (U.S. Patent No. 6,782,103) – discloses cryptographic key management. Arthan et al. teaches a private key and public key pair where the private key is encrypted for delivery using a key encryption key (KEK) and stored in an encrypted state at a source computer 1, where it is decrypted whenever it is needed for use in the transmission of data. See *Arthan et al.* at col. 2, lines 40-48. Arthan et al. suggests that a source system 1 uses a private key (DSPR) to protect data flowing from the source system 1 to a destination system 2. *Id.* at col. 1, lines 58-67.

More specifically, Arthan et al. teaches that a central system 5 generates private and public keys. *Id.* at col. 3, lines 38-41. After the keys are generated, the private key (DSPR) is transmitted by the central system 5 to the source system 1, and the corresponding public key (DSPU) is transmitted by the central system 5 to the destination system 2. *Id.* at col. 3, lines 25-41. The destination system 2 can also be supplied in advance with a spare version of the public key. *Id.* at col. 4, lines 15-20. When the private key needs to be changed, such as in the event of a compromise, the version of the private key corresponding to the spare public key can be put into immediate use in the source system 1 as soon as it is supplied. *Id.* at col. 4, lines 20-23. Since the public and private keys are generated in pairs, the spare private key corresponding to the spare public key will "need to be held securely after generation and then called up as required." *Id.* at col. 4, lines 25-32.

Notably, Arthan et al. does not provide any further detail regarding how the spare private key is held securely and does not provide any suggestion that such a spare private key is output from the central system 5 prior to being used. Because Arthan et al. discloses that the central system 5 delivers the keys to the source and destination systems 1 and 2, it seems to Applicants to suggest that the spare private key is stored by the central system 5 until it is supplied from the central system 5 to the source system 1 for use. Accordingly, Arthan et al. suggests a central system 5 that generates first and second key pairs, retains the spare private key, and outputs the active private key to the source system 1 and the active and spare public keys to the destination system 2.

Kurn et al. (U.S. Publication No. 2002/0071561) – discloses a method and apparatus for enforcing the separation of computer operations and business management roles in a cryptographic system. According to Kurn et al., a key repository process 20 stores one or more entries defining Operators and two or more entries defining Owners in a database 30. *Kurn et al.* at ¶ [0076]. An integrity key 22 is configured to ensure the integrity of sensitive information within the database 30. *Id.* Each Owner entry retains a share of a protection key 24 configured to protect sensitive information on the database 30. *Id.* The database 30 also stores enterprise credentials 32. *Id.* Crucial information in the database 30 is protected against modification by the integrity key 22, while confidential data is protected by the protection key 24. *Id.* at ¶ [0091]. When the key repository process 20 is restarted, an operator known to the system exposes the integrity key 22 by use of the correct identity and password. *Id.* The protection key 24 is assembled from a set of secrets that are split among the multiple Owners. *Id.* When the requisite number of Owners have exposed their share of the split protection key 24, the protection key can be recovered. *Id.*

B. Differences Between Claimed Invention and Prior Art

Claim 50, as amended herein recites, "a processor configured to: generate a first private key and corresponding first public key; generate a second private key associated with the first private key; and create a second public key corresponding to the second private key; a storage medium coupled to the processor, the storage medium configured to store the first private key; and a transmitter coupled to the processor to: output the second private key such that it is not

stored in the storage medium, the second private key being output as a plurality of shares to a plurality of different entities once, such that the second private key can be re-created and used when there is no access to the first private key, wherein the first private key is disabled when the second private key is re-created and used for authentication; and output the first public key and the second public key to a verifier device; wherein the processor uses the stored first private key for authentication of the mobile user device prior to using the second private key."

The Office Action fails to characterize any particular device between the source system 1, destination system 2 and central system 5 as corresponding to the single device claimed in independent claim 50. Applicants will therefore refer to each of these devices and why they fail to teach or suggest the limitations recited in independent claim 50.

The central system 5 appears to Applicants to be the most relied on by the Office Action. As noted, the central system 5 generates an active private and public key pair and a spare private and public key pair. See *Arthan et al.* at col. 3, lines 38-41; and col. 4, lines 15-20. The central system 5 then outputs the active private key to the source system 1, and the active public key and spare public key to the destination system 2. *Id.* at col. 3, lines 25-41; col. 4, lines 15-20. It appears from Arthan et al. that the central system 5 securely stores the spare private key for future deployment to the source system 1. *Id.* at col. 4, lines 25-32.

Given such teachings by Arthan et al., the central system 5 is actually contrary in some respects to the device recited in independent claim 50. For example, the central system 5 generates the active private key, and then outputs the active private key to the source system 1 for active use. This is exactly opposite to claim 50, where the processor uses the stored first private key for authentication of the mobile user device. In other words, the central system 5 outputs the active private key, which is then used before the spare private key, while the device of claim 50 stores the first private key and uses the stored first private key for authentication before using the output second private key.

Another difference is the fact that the central system 5 does not appear to use any of the keys for authentication of the central system 5. Instead, it just generates the keys and then sends them off to other devices for use by these other devices. In view of the forgoing, central system 5 fails to include "a storage medium coupled to the processor, the storage medium configured to **store the first private key**; and a transmitter coupled to the processor to: **output the second**

private key such that it is not stored in the storage medium … wherein the processor **uses the stored first private key for authentication** of the mobile user device **prior to using the second private key**," as recited in independent claim 50.

Turning now to the source system 1, Arthan et al. suggests that the source system 1 simply receives the active private key from the central system 5 (*Id.* at col. 3, lines 25-41; col. 4, lines 15-20) and stores the private key into a volatile memory for use (*Id.* at col. 2, lines 48-50). This source system 1 also fails to include all of the limitation of independent claim 50. For example, in addition to not generating any keys, the source system 1 apparently fails to include a transmitter coupled to the processor to "output [a] second private key such that it is not stored in the storage medium."

Turning now to the destination system 2, Arthan et al. suggests that the destination system 2 simply receives the public keys from the central system 5. Among other features (e.g., generating keys, etc.), the destination system 2 does not appear to store a private key, output a private key, or use a private key.

Accordingly, none of the devices in Arthan et al. includes a storage medium configured to "**store the first private key**"; a transmitter to "**output the second private key** such that it is not stored in the storage medium," and a processor that "**uses the stored first private key for authentication** of the mobile user device prior to using the second private key."

Furthermore, Applicants assert that Kurn et al. fails to remedy these deficiencies of Arthan et al., and that the combination of Kurn et al. with Arthan et al. in the way suggested by the Examiner would result in a complete failure of Arthan et al. Indeed, the central system 5 of Arthan et al. is the only device which outputs any private keys. However, since the private key output by the central system 5 is the active private key, it would be contrary to the teachings of Kurn et al. That is, if the central system 5 output the active private key in shares to multiple users, where no single user alone could use the key, then the source system 1 would be unable to even use the private key output by the central system 5. Therefore, in addition to not remedying the deficiencies of Arthan et al., a person of ordinary skill in the art would be motivated not to combine Kurn et al. with Arthan et al. in the manner asserted by the Examiner.

Applicants respectfully assert that Arthan et al. and Kurn et al., when combined, do not teach or suggest at least "a storage medium coupled to the processor, the storage medium

configured to **store the first private key**; and a transmitter coupled to the processor to: **output the second private key** such that it is not stored in the storage medium, the second private key being output as a plurality of shares to a plurality of different entities once, such that the second private key can be re-created and used when there is no access to the first private key, wherein the first private key is disabled when the second private key is re-created and used for authentication; … wherein the processor **uses the stored first private key** for authentication of the mobile user device **prior to using the second private key**," as recited in independent claim 50, and these differences between claim 50 and the combined teachings of the cited references would not have been obvious to one of ordinary skill in the art at the time the invention was made. Applicants, therefore, respectfully request that the Examiner withdraw the 35 U.S.C. § 103(a) obviousness rejection to claim 50.

Furthermore, the nonobviousness of independent claim 50 precludes a rejection of claim 56, which depends therefrom, because a dependent claim is obvious only if the independent claim from which it depends is obvious. *See In re Fine*, 5 U.S.P.Q.2d 1596, 1600 (Fed. Cir. 1988), *see also* MPEP § 2143.03. Therefore, Applicants request that the Examiner withdraw the 35 U.S.C. § 103(a) obviousness rejection to claim 56, in addition to the rejection to independent claim 50.

Claims 1-3, 5-9, 11-14, 16-24, 26-28, 51 and 53-55

The Office Action rejected claims 1-3, 5-9, 11-14, 16-24, 26-28, 51 and 53-55 under 35 U.S.C. §103(a) as being allegedly obvious over U.S. Patent No. 6,782,103 (hereinafter "Arthan et al.") in view of U.S. Publication No. 2002/0071561 (hereinafter "Kurn et al."), and further in view of U.S. Publication No. 2002/0018570 (hereinafter "Hansmann et al."). These rejections are respectfully traversed in their entirety.

Applicants respectfully submit that claims 1-3, 5-9, 11-14, 16-24, 26-28, 51 and 53-55 are not obvious in view of the cited references under a *Graham* analysis. More specifically, the combination of Arthan et al., Kurn et al. and Hansmann et al. fails to teach or suggest all of the limitations of claims 1-3, 5-9, 11-14, 16-24, 26-28, 51 and 53-55, and one of ordinary skill in the art would not arrive at the limitations of claims 1-3, 5-9, 11-14, 16-24, 26-28, 51 and 53-55 in view of the differences between these references and the presented claims.

A. Scope of the Prior Art

Arthan et al. (U.S. Patent No. 6,782,103) – discloses cryptographic key management, as summarized hereinabove with reference to the rejections of claims 50 and 56.

Kurn et al. (U.S. Publication No. 2002/0071561) – discloses a method and apparatus for enforcing the separation of computer operations and business management roles in a cryptographic system, as summarized hereinabove with reference to the rejections of claims 50 and 56.

Hansmann et al. (U.S. Publication No. 2002/0018570) – discloses a simplified authentication system for communicating devices having fewer security requirements than conventional cryptographic systems. *Hansmann et al.* at Abstract. The device to be authenticated includes a secret, a function component for generating a random number, a function component for exchanging messages with other devices and finally an algorithm for calculating a hash using random number and secret. *Id.* The device requesting authentication includes a secret and an algorithm for calculating a hash using a random number received from the device to be authenticated. *Id.* A function component for comparing both hashes may be implemented in both devices. *Id.* If the hashes calculated by both devices match it can be assumed that the authentication was successful. *Id.* Instead of using the digital keys and conventional symmetric or asymmetric algorithms, Hansmann et al. contemplates using a relatively simple random number and a simple hash algorithm, which sufficiently fulfills the security requirements of many communication architectures. *Id.*

B. Differences Between Claimed Invention and Prior Art

Claims 1-3, 5-9, 14, 16-18, 22-24 and 53-55

Claim 1 recites in part "outputting the second private key from the mobile user device such that it is not stored on the mobile user device while retaining the first private key in the mobile user device, wherein outputting the second private key comprises transmitting a plurality of shares of the second private key from the mobile user device to a plurality of different entities once, such that the second private key can be re-created and used when the first private key is

inaccessible; transmitting the first public key and the second public key to a verifier device; and using the retained first private key for authentication of the mobile user device prior to using the second private key."

As noted above regarding independent claim 50, the central system 5 of Arthan et al. generates an active private and public key pair and a spare private and public key pair. See *Arthan et al.* at col. 3, lines 38-41; and col. 4, lines 15-20. The central system 5 then outputs the active private key to the source system 1, and the active public key and spare public key to the destination system 2. *Id.* at col. 3, lines 25-41; col. 4, lines 15-20. It appears from Arthan et al. that the central system securely stores the spare private key for future deployment to the source system 1. *Id.* at col. 4, lines 25-32.

Such a central system 5 is contrary in at least some respects to the recitations in independent claim 1. In claim 1, the **retained** private key is used for authentication prior to using the output private key. In the central system 5, the **output** private key is used by the source system 1 prior to using the stored spare private key.

In addition, the central system 5 that creates the first and second key pairs does not appear to actually use any of the keys for authentication of the central system 5. Instead, it just generates the keys and then sends them off to other devices for use by these other devices. This is contrary to claim 1, where the first and second private keys and first and second public keys are created at the mobile user device, and the retained first private key is used for authentication of the mobile user device.

Arthan et al. also does not teach or suggest the source system 1 or the destination system 2 as performing any steps relating to outputting one private key while retaining another private key and using the retained private key for authentication. Accordingly, Arthan et al. fails to teach of suggest "**outputting the second private key** from the mobile user device such that it is not stored on the mobile user device **while retaining the first private key** in the mobile user device," and "**using the retained first private key** for authentication of the mobile user device **prior to using the second private key**," as recited in independent claim 1.

Furthermore, neither Kurn et al. nor Hansmann et al. include any teachings or suggestions to remedy these deficiencies of Arthan et al.

Applicants respectfully assert that Arthan et al., Kurn et al. and Hansmann et al., when combined, do not teach or suggest at least "**outputting the second private key from the mobile user device such that it is not stored on the mobile user device while retaining the first private key in the mobile user device**, wherein outputting the second private key comprises transmitting a plurality of shares of the second private key from the mobile user device to a plurality of different entities once, such that the second private key can be re-created and used when the first private key is inaccessible; transmitting the first public key and the second public key to a verifier device; and **using the retained first private key for authentication** of the mobile user device **prior to using the second private key**," as recited in independent claim 1 and as similarly recited in independent claim 14, and these differences between claims 1 and 14 and the combined teachings of the cited references would not have been obvious to one of ordinary skill in the art at the time the invention was made. Applicants, therefore, respectfully request that the Examiner withdraw the 35 U.S.C. § 103(a) obviousness rejection to claims 1 and 14.

Similarly, Arthan et al., Kurn et al. and Hansmann et al., when combined, do not teach or suggest at least "**retain the first private key and output the second private key** such that it is not stored on a device where the second private key was created, the second private key being output as a plurality of shares to a plurality of different entities once such that the second private key can be re-created and used when there is no access to the first private key, wherein the first private key is disabled when the second private key is re-created and used for authentication; output the first public key and the second public key to a verifier device; and **use the retained first private key for authentication prior to using the second private key for authentication**," as recited in independent claim 22, and these differences between claim 22 and the combined teachings of the cited references would not have been obvious to one of ordinary skill in the art at the time the invention was made. Applicants, therefore, respectfully request that the Examiner withdraw the 35 U.S.C. § 103(a) obviousness rejection to claim 22.

Furthermore, the nonobviousness of independent claims 1, 14 and 22 precludes a rejection of claims 2, 3, 5-10, 15-18, 23, 24 and 53-55, which depend therefrom, because a dependent claim is obvious only if the independent claim from which it depends is obvious. *See In re Fine*, 5 U.S.P.Q.2d 1596, 1600 (Fed. Cir. 1988), *see also* MPEP § 2143.03. Therefore,

Applicants request that the Examiner withdraw the 35 U.S.C. § 103(a) obviousness rejection to claims 2, 3, 5-10, 15-18, 23, 24 and 53-55, in addition to the rejection to independent claims 1, 14 and 22.

Claims 11-13, 19-21, 26-28 and 51

Claim 11, as currently amended, recites, "receiving a first public key from a mobile user device **wherein the first public key has a corresponding first private key stored on the mobile user device**; receiving a second public key from the mobile user device, the second public key associated with the first public key, wherein the second public key has a corresponding second private key that is split into a plurality of shares that are sent to a plurality of different entities such that it is not stored on the mobile user device, where each share is sent only once and to a different entity, such that the second private key can be re-created and used when there is no access to a first private key corresponding to the first public key, wherein the first private key is disabled when the second private key is re-created and used for authentication; **using the first public key for authentication** of the mobile user device; and **using the second public key for authentication if the first public key fails**."

As noted above, Arthan et al. teaches the use of private and public key pairs, and the use of a spare public key. However, the Examiner is again mixing the different systems from Arthan et al. so that both the central system 5 and the source system 1 are characterized as the mobile user device of claim 11 at the same time. Applicants assert that such a characterization is improper and contrary the actual teachings of Arthan et al. as a whole.

Arthan et al. teaches that the destination system 2 receives the active public key from the central system 5. Further, the central system 5 outputs the active private key to the source system 1 for use in encrypting data from the source system 1. Therefore, if the central system 5 is characterized as the mobile user device of claim 11, then there is no teaching or suggestion of the first public key having a corresponding first private key stored on the central system 5, where the first public key is used for authentication of the central system 5. Similarly, if the source system 1 is characterized as the mobile user device of claim 11, then there is no teaching or suggestion of receiving the first public key from the source system 1 or receiving the second public key from the source system 1.

Furthermore, neither Kurn et al. nor Hansmann et al. include any teachings or suggestions to remedy these deficiencies of Arthan et al.

Applicants respectfully assert that Arthan et al., Kurn et al. and Hansmann et al., when combined, do not teach or suggest at least "receiving a first public key from a mobile user device **wherein the first public key has a corresponding first private key stored on the mobile user device**; receiving a second public key from the mobile user device, the second public key associated with the first public key, wherein the second public key has a corresponding second private key that is split into a plurality of shares that are sent to a plurality of different entities such that it is not stored on the mobile user device, where each share is sent only once and to a different entity, such that the second private key can be re-created and used when there is no access to a first private key corresponding to the first public key, wherein the first private key is disabled when the second private key is re-created and used for authentication; **using the first public key for authentication** of the mobile user device; and **using the second public key for authentication if the first public key fails**," as recited in independent claim 11, and as similarly recited in independent claims 19, 26 and 51, and these differences between claims 11, 19, 26 and 51 and the combined teachings of the cited references would not have been obvious to one of ordinary skill in the art at the time the invention was made. Applicants, therefore, respectfully request that the Examiner withdraw the 35 U.S.C. § 103(a) obviousness rejection to claims 11, 19, 26 and 51.

Furthermore, the nonobviousness of independent claims 11, 19 and 26 precludes a rejection of claims 12, 13, 20, 21, 27 and 28, which depend therefrom, because a dependent claim is obvious only if the independent claim from which it depends is obvious. *See In re Fine*, 5 U.S.P.Q.2d 1596, 1600 (Fed. Cir. 1988), *see also* MPEP § 2143.03. Therefore, Applicants request that the Examiner withdraw the 35 U.S.C. § 103(a) obviousness rejection to claims 12, 13, 20, 21, 27 and 28, in addition to the rejection to independent claims 11, 19, 26 and 51.

Claims 10 and 15

The Office Action rejected claims 10 and 15 under 35 U.S.C. §103(a) as being allegedly obvious over U.S. Patent No. 6,782,103 (hereinafter "Arthan et al.") in view of U.S. Publication No. 2002/0071561 (hereinafter "Kurn et al."), in view of U.S. Publication No. 2002/0018570

(hereinafter "Hansmann et al."), and further in view of Official Notice. These rejections are respectfully traversed in their entirety.

Claims 10 and 15 depend from claims 1 and 14, respectively. As noted previously, the combination of Arthan et al., Kurn et al., and Hansmann et al. fail to teach or suggest all of the limitations of independent claims 1 and 14. The nonobviousness of independent claims 1 and 14 precludes a rejection of claims 10 and 15, which depend therefrom, because a dependent claim is obvious only if the independent claim from which it depends is obvious. *See In re Fine*, 5 U.S.P.Q.2d 1596, 1600 (Fed. Cir. 1988), *see also* MPEP § 2143.03. Therefore, Applicants request that the Examiner withdraw the 35 U.S.C. § 103(a) obviousness rejection to claims 10 and 15.

Claims 57-68

The Office Action rejected claims 57-68 under 35 U.S.C. §103(a) as being allegedly obvious over U.S. Patent No. 6,782,103 (hereinafter "Arthan et al.") in view of U.S. Patent No. 6,009,177 (hereinafter "Sudia"). These rejections are respectfully traversed in their entirety.

Applicants respectfully submit that claims 57-68 are not obvious in view of the cited references under a *Graham* analysis. More specifically, the combination of Arthan et al. and Sudia fails to teach or suggest all of the limitations of claims 57-68, and one of ordinary skill in the art would not arrive at the limitations of claims 57-68 in view of the differences between these references and the presented claims.

A. Scope of the Prior Art

Arthan et al. (U.S. Patent No. 6,782,103) – discloses cryptographic key management, as summarized hereinabove with reference to the rejections of claims 50 and 56.

Sudia (U.S. Patent No. 6,009,177) – discloses a cryptographic system and method with a key escrow feature for verifiably splitting users' private encryption keys into components and for sending those components to trusted agents. For example, Sudia describes an embodiment in which the device includes a chip that breaks the private key into several pieces and forms a share packet for each trustee or escrow agent designated by the user. (col. 18, lines 12-26). It appears to Applicants from the disclosure in Sudia, that the purpose of keeping the private key with the

trustee or escrow agent in Sudia is to verify that the user device is a trusted device and to provide a signed certificate from the master escrow center to be used for communications between devices (see, e.g., col. 20, lines 26-35), and to allow access to the private key by law enforcement for the ability to intercept and decrypt communication to and from a particular user (see, e.g., col. 30, lines 5-19). Applicants are not able to find disclosure, nor has the Examiner identified any disclosure, in Sudia describing the output of one private key and the retention of another private key at the user device. Instead, the only existing private key for the chip is both transmitted to the plurality of different entities and retained stored on the chip for subsequent use by the user device after it is transmitted to the trustee or escrow agent. (col. 17, lines 62-63).

B. Differences Between Claimed Invention and Prior Art

Independent claim 57 recites "re-creating a second private key **at a mobile user device that has no access to a first private key associated with the second private key**, wherein the second private key is re-created using at least some shares of a plurality of shares of the second private key located at a plurality of different entities; creating a third private key and a corresponding third public key; **outputting the third private key from the mobile user device such that it is not stored on the mobile user device while retaining the second private key at the mobile user device**; and using the second private key for authentication of the mobile user device." Independent claims 61 and 65 also include similar recitations.

In the response to arguments, the Office Action asserts that "Arthan teaches that the spare private key is used when the current private key is compromised (column 4, lines 15-22). To one of ordinary skill in the art, it would have been obvious that a compromise would include having the private key stolen. Therefore, Arthan teaches that the spare key is used when there is no access to the first private key." See *Final Office Action* at p. 3. Applicants assert that the Examiner has mischaracterized the technology with relation to a stolen key. In particular, to a person of ordinary skill in the art, a stolen key refers to a key that has been copied, not taken and erased from the original device. As such, a stolen key will still be accessible to the original device. If the Examiner intends to continue asserting that a stolen key is erased from the original device, Applicants request that the Examiner provide evidence to support such an assertion.

Furthermore, Arthan et al. itself appears to suggest that a compromised private key refers to a private key that is left on the compromised device. For example, the teachings in Arthan et al. suggest that a compromised private key refers to the private key being cracked or accessed by an unintended party. See, *e.g.*, *Arthan et al.* at col. 3, lines 19-24; and col. 5, lines 30-35. However, merely being cracked or accessed does not suggest that the compromised private key is erased from the compromised device. Indeed, there does not appear to be any teaching or suggestion that a compromised private key means that the private key is not accessible to a device using the compromised private key. As Arthan et al. fails to provide any such disclosure, Arthan et al. still fails to teach or suggest "re-creating a second private key at a mobile user device that has no access to a first private key."

In addition, Arthan et al. does not teach or suggest outputting a third private key while retaining a second private key. Instead, Arthan et al. teaches that the active private key is output and used before the spare private key is output. Accordingly, Arthan et al. fails to teach or suggest "outputting the third private key from the mobile user device such that it is not stored on the mobile user device while retaining the second private key at the mobile user device; and using the second private key for authentication of the mobile user device before using the third private key."

Furthermore, Applicants assert that Sudia fails to remedy these deficiencies of Arthan et al. with respect to independent claims 57, 61 and 65.

Applicants respectfully assert that Arthan et al. and Sudia, when combined, do not teach or suggest at least "re-creating a second private key **at a mobile user device that has no access to a first private key associated with the second private key**, wherein the second private key is re-created using at least some shares of a plurality of shares of the second private key located at a plurality of different entities; creating a third private key and a corresponding third public key; **outputting the third private key from the mobile user device such that it is not stored on the mobile user device while retaining the second private key at the mobile user device**; and using the second private key for authentication of the mobile user device," as recited in independent claim 57, and as similarly recited in independent claims 61 and 65, and these differences between claims 57, 61 and 65 and the combined teachings of the cited references would not have been obvious to one of ordinary skill in the art at the time the invention was

made. Applicants, therefore, respectfully request that the Examiner withdraw the 35 U.S.C. § 103(a) obviousness rejection to claims 57, 61 and 65.

Furthermore, the nonobviousness of independent claims 57, 61 and 65 precludes a rejection of claims 58-60, 62-64 and 66-68, which depend therefrom, because a dependent claim is obvious only if the independent claim from which it depends is obvious. *See In re Fine*, 5 U.S.P.Q.2d 1596, 1600 (Fed. Cir. 1988), *see also* MPEP § 2143.03. Therefore, Applicants request that the Examiner withdraw the 35 U.S.C. § 103(a) obviousness rejection to claims 58-60, 62-64 and 66-68, in addition to the rejection to independent claims 57, 61 and 65.

Should any of the above rejections be maintained, Applicant respectfully requests that the noted limitations be identified in the cited references with sufficient specificity to allow Applicant to evaluate the merits of such rejections. In particular, rather than generally citing whole sections or columns, Applicant requests that the each claimed element be specifically identified in the prior art to permit evaluating the references.

CONCLUSION

In light of the amendments contained herein, Applicant submits that the application is in condition for allowance, for which early action is requested.

Please charge any fees or overpayments that may be due with this response to Deposit Account No. 17-0026.

Respectfully submitted,

Dated: March 14, 2011

By: /Won Tae C. Kim/
Won Tae C. Kim, Reg. # 40,457
(858) 651 6295

QUALCOMM Incorporated
5775 Morehouse Drive
San Diego, California 92121
Telephone: (858) 658-5787
Facsimile: (858) 658-2502